Notice of Allowability	Application No.	Applicant(s)	
	09/905,342	SCHMALL ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☐ This communication is responsive to _____.

2. ☒ The allowed claim(s) is/are *1-20*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Attorney Samir Bhavsar on 01 February 2006. The application has been amended as follows:

Please amend the following:

13. (**Currently Amended**) ~~A computer data signal embodied in a transmission medium which embodies instructions~~ **Instructions embodied in a computer readable medium and** executable by a computer for detecting a class of viral code, **the instructions** comprising:

a first segment including heuristic analyzer code to:

heuristically analyze a subject file to **detect at least one class of viral code, the heuristic analysis based at least in part on one or more rules;**

identify at least one new characteristic of a viral code;

generate at least one new rule, the at least one new rule based at least in part on the at least one new characteristic;

generate a set of flags **based at least in part on the heuristic analysis** ~~along with statistical information~~;

and

a second segment including scanner code using the set of flags ~~with statistical information~~ to perform at least one search for a scan string and/or a statement type in the subject file, and triggering a positive detection alarm if each of the at least one search is found at least a corresponding predetermined number of times.

DETAILED ACTION

2. Claims 1,5, and 11-17 have been amended.

3. Claim 20 has been added.

4. Claims 1-20 are pending.

Response to Arguments

5. Applicant's arguments filed 17 November 2005 have been fully considered and they are persuasive.

Allowable Subject Matter

6. Claims **1-20** are allowed.

7. The following is an examiner's statement of reasons for allowance: The present invention is directed towards a method and system for detecting a class of viral code by using a series of techniques including heuristic analysis of a subject computer code, use of statistical information, and use of search/string operation. Combining these techniques enables classification of viral code to be efficient. Each independent claim identifies the uniquely distinct features "**detecting at least one class of viral code, the heuristic analysis based at least in part on one or more rules, identifying at least one new characteristic of a viral code, generating at least one new rule, and**

generating a set of flags based at least in part on the heuristic analysis". The closest prior art, Nachenberg (U.S. Patent No. 5,826,013) discloses a module for detecting polymorphic viruses by emulating instructions of a computer program, either singularly or in combination, fail to anticipate or render the above underlined limitations obvious.

8. Therefore, **claims 1 and 11-14** and the respective **dependent claims 2-10 and 15-19** are in condition for allowance.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cdf
February 3, 2006

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137